SHOOK, HARDY & BACON L.L.P.
Erin L. Leffler (PA ID No. 204507)
Two Commerce Square
2001 Market St., Suite 3000
Philadelphia, PA 19103
Telephone: (215) 278-2555
Facsimile: (215) 278-2594
eleffler@shb.com

Attorneys for Defendants Cabela's L.L.C. and BPS Direct, L.L.C.

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF PENNSYLVANIA

DAVID IRVIN, individually and on behalf of all others similarly situated, Plaintiff, v. CABELA'S L.L.C., *et al.*, Defendants.	Case No. 1:23-cv-00530-CCC

DEFENDANTS' MEMORANDUM OF LAW IN SUPPORT OF THEIR MOTION TO DISMISS PLAINTIFF'S AMENDED CLASS ACTION COMPLAINT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Rules

INTRODUCTION

Plaintiff asserts this putative class action against Defendants Cabela's L.L.C. and BPS Direct, L.L.C. (collectively, "BPS"). Plaintiff alleges that when he purchased a firearm from cabelas.com, information about his website visit was disclosed to Facebook, including his name, address, Facebook ID, and the type of gun he purchased. Plaintiff alleges this information was disclosed because BPS utilized Facebook's "pixel" technology on its website, and that BPS should therefore be subject to liability because it did not obtain his consent to share the information. As discussed below, this theory suffers from several defects that require dismissal of the Complaint in its entirety under Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6).

Plaintiff alleges he is a Facebook user. It is widely known that Facebook collects data about its users' browsing activities on the Internet. Like all Facebook users, Plaintiff agreed to Facebook's Terms of Service and Privacy Policy, which permit Facebook to collect information about his interactions with websites across the Internet, and which disclose that Facebook uses cookies, pixels, and other technologies to collect information about websites they visit. *See* Facebook's Terms of Service, available at https://www.facebook.com/terms. As a result, when Plaintiff visited third-party websites that include Facebook code, his browser sent Facebook the URL of the page he visited along with his Facebook ID. This is an entirely

ordinary part of Internet commerce; BPS's websites include the same code that is present on countless websites.

Despite his consent to these disclosures (not to mention BPS's Privacy Policy), Plaintiff seeks to hold BPS liable for its limited role in Facebook's accumulation of user data. Plaintiff filed the Amended Complaint on June 16, 2023,[1] which asserts claims under Pennsylvania's Wiretapping and Electronic Surveillance Control Act and Uniform Firearms Act. Both claims fail, for several reasons.

First, Plaintiff **lacks Article III standing** because he has not alleged an injury in fact. As both the Supreme Court and courts in the Third Circuit have recognized, allegations of a "bare procedural violation" of a statute is insufficient to establish standing. *Barclift v. Keystone Credit Servs., LLC*, 585 F. Supp. 3d 748 (E.D. Pa. 2022); *see also TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2204–07 (2021). But that is all Plaintiff alleges here. Indeed, Plaintiff has built his case around the pre-*TransUnion* theory that a bare statutory violation is enough. And it is obvious why: Plaintiff could not possibly have been harmed by Facebook's access to the very information he agreed it could collect.

Second, Plaintiff's claim under Pennsylvania's **Wiretapping and Electronic Surveillance Control Act ("WESCA")** should be dismissed because Plaintiff does

[1] BPS moved to dismiss Plaintiff's Complaint on May 26, 2023. Dkt. 13. Instead of responding to BPS's substantive arguments, Plaintiff amended his Complaint. Dkt. 20.

not assert that the alleged interception took place in Pennsylvania. Plaintiff also fails to allege several key elements under the statute, including that BPS intercepted the "contents" of his communications, or that a pixel is "device." Lastly, and more fundamentally, Plaintiff consented to any supposed "interception" both when he agreed to Facebook's terms and conditions and to BPS's Privacy Policy.

Third, Plaintiff's claim under the **Uniform Firearms Act** ("UFA") should be dismissed. The UFA relates exclusively to the sale or transfer of firearms—including its confidentiality provision. Yet, Plaintiff fails to allege an improper "disclosure" by BPS because the Complaint does not clearly identify *who* (BPS, Facebook, or Plaintiff's own browser) allegedly disclosed Plaintiff's communications with BPS. And even if Plaintiff had alleged a "disclosure," he does not allege a "public" disclosure as required by the statute.

The Complaint should be dismissed in its entirety.

BACKGROUND

BPS is a nationwide retailer of outdoor products, including camping, hunting, and other outdoor equipment. First Am. Compl. ("FAC") ¶¶ 7, 8. Plaintiff David Irvin alleges he is a Pennsylvania citizen who purchased a Henry Big Boy Classic Centerfire Lever-Action Rifle - .45 from cabela's.com on December 2, 2021. *Id.* ¶ 6. Plaintiff claims that BPS "assisted Facebook" with "intercepting" his communications by use of the Meta Pixel. *Id.* ¶ 9. According to Plaintiff, BPS

configured the pixel to transmit (1) the URLs of webpages visited, including "when users access pages for particular products" and the "title and description of the webpage"; (2) certain buttons users click, such as "Order Online," "Add to Cart," and "Check Out"; and (3) information purchasers enter into online form fields. *Id.* ¶¶ 17–24. These communications allegedly contained "personally identifiable information" and information about "firearm purchases." *Id.* ¶ 9. Separately, Plaintiff alleges that the pixel "compels the user's browser" to send Facebook any Facebook cookies stored on the user's browser. *Id.* ¶ 28.

LEGAL STANDARD

To survive a Rule 12(b)(6) motion to dismiss, a complaint's "[f]actual allegations must be enough to raise a right to relief above the speculative level." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). A complaint does not "suffice if it tenders naked assertions devoid of further factual enhancement." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citation omitted). Rather, the "complaint must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." *Id.* (cleaned up). This demands "more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Twombly*, 550 U.S. at 570.

ARGUMENT

I. Plaintiff Lacks Standing to Assert His Claims.

Plaintiff lacks standing to bring all of his claims because he has not alleged an actual injury. His Amended Complaint is simply silent on how he was affected by any disclosure of his data to Facebook. That is no surprise, because Plaintiff consented to the very practices he is complaining about by agreeing to Facebook's terms and Cabela's privacy policies.

To establish standing, Plaintiff has the burden of establishing "(1) an injury-in-fact; (2) that is fairly traceable to the defendant's challenged conduct; and (3) that is likely to be redressed by a favorable judicial decision." *St. Pierre v. Retrieval-Masters Creditors Bureau, Inc.*, 898 F.3d 351, 356 (3d Cir. 2018) (citing *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 590 (1992)). To establish injury in fact, Plaintiff must show that he has suffered a "concrete" and "particularized" injury, which must be "actual or imminent, not conjectural or hypothetical." *Burris v. Weltman, Weinberg & Reis, Co., L.P.A.*, 2022 WL 3580766, at *2 (M.D. Pa. Aug. 19, 2022). The "concrete harm" prong is not automatically satisfied merely because "a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right." *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2205 (2021). "Only those plaintiffs who have been concretely harmed by a defendant's statutory violation may sue that private defendant over that violation in federal court." *Id.* (emphasis added).

Authority from the Third Circuit is in accord. For example, in *Barclift v. Keystone Credit Servs., LLC*, 585 F. Supp. 3d 748 (E.D. Pa. 2022), the plaintiff alleged that her "right not to have her private information shared with third parties is concrete injury sufficient to confer standing." *Id.* at 760. The court disagreed, because the plaintiff had not "back[ed] up her conclusory statement with any facts of how or why the alleged harm is concrete." *Id.* As a result, the court held that plaintiff's allegations of a "bare procedural violation of the FDCPA" did not satisfy the plaintiff's burden of establishing standing. *Id.*

Other courts in the Third Circuit have issued similar rulings. *See, e.g.*, *Burris*, 2022 WL 3580766, at *6 (dismissing claim for lack of standing because the plaintiff "simply seeks damages based on the fact that Defendant" violated a statute); *Coulter v. AR Res., Inc.*, 2023 WL 3182938, at *3 (M.D. Pa. May 1, 2023) (adopting *Burris* and rejecting the plaintiff's argument that "the dissemination of her personal information alone is enough to constitute similar harm to common law damages associated with invasion-of-privacy torts").

Thus, both *TransUnion* and courts in the Third Circuit agree: a bare statutory violation is simply not enough to establish standing. But that is all that Plaintiff alleges here. Indeed, the only claimed injury is BPS's alleged statutory violation. Compl. ¶ Prayer for Relief, e–f. Plaintiff asserts no other allegations of harm—not

even conclusory ones. *See TransUnion*, 141 S. Ct. at 2214 ("an asserted informational injury that causes no adverse effects does not satisfy" standing).

To be sure, the Third Circuit has recognized that the invasion of privacy can, in some circumstances, be a concrete injury. *See, e.g.*, *Burris*, 2022 WL 3580766, at *7. But under Pennsylvania law, an invasion of privacy requires "publicity," which means "a matter must be made public through communication to either the general public or enough people that the matter is 'substantially certain' to become public knowledge." *Perloff v. Transamerica Life Ins. Co.*, 393 F. Supp. 3d 404, 409–10 (E.D. Pa. 2019) (quoting the Restatement (Second) of Torts § 652D, cmt. a, which Pennsylvania courts have adopted). Disclosure of private facts "to one person or a small group of people does not meet this standard." *Id.* (citing *Vogel v. W. T. Grant Co.*, 458 Pa. 124, 327 A.2d 133, 137–38 (1974)).

Here, Plaintiff only alleges that his information was disclosed to a single entity, Facebook. *See, e.g.*, FAC ¶¶ 9, 17. That is hardly a communication to the "public at large" or to "so many persons that [it is] substantially certain to become one of public knowledge" as the law requires. *Burris*, 2022 WL 3580766, at *7 ("Without publicity, Plaintiff cannot establish that he suffered the type of harm recognized by such a cause of action—and without that harm, Plaintiff has no common law analogue upon which to assert standing."). As the court recognized in *Barclift*, the plaintiff's alleged "right not to have her private information shared with

third parties" did "not bear a close enough relationship to the tort of disclosure of private facts for one major reason—*there was no publicity*. 585 F. Supp. 3d at 758 (emphasis in original). The same is true here.[2]

Plaintiff also lacks standing to seek an injunction, which is only appropriate to protect against future harm. Here, Plaintiff does not, *and cannot*, allege that he will visit cabelas.com without knowledge that the site employs pixel technology. As such, he lacks standing to pursue a claim for injunctive relief. *See, e.g.*, *Silva v. Rite Aid Corp.*, 416 F. Supp. 3d 394, 400 (M.D. Pa. 2019) (dismissing a claim for injunctive relief because the intent to purchase supplements does not alone establish a future injury); *McNair v. Synapse Grp. Inc.*, 672 F.3d 213, 225–26 (3d Cir. 2012) (dismissing a claim for injunctive relief because plaintiffs cannot establish any reasonable likelihood of future injury).

Plaintiff's Petition should be dismissed for lack of standing.

II. Plaintiff Fails to Adequately Allege a Violation of the WESCA.

Pennsylvania's WESCA prohibits a person from "intentionally . . . procur[ing] any other person to intercept or endeavor to intercept any wire, electronic or oral communication." 18 Pa.C.S. § 5703(1). To state a WESCA claim, Plaintiff must allege an "interception," which the Act defines as an "acquisition of the contents of

[2] Nor *could* Plaintiff claim any injury, because as discussed below, Plaintiff (like every Facebook user) agreed to be governed by Facebook's privacy policies, and was put on notice of BPS's Privacy Policy.

any wire, electronic or oral communication through the use of any electronic, mechanical or other device." 18 Pa.C.S. § 5702 (emphasis added). Plaintiff alleges that BPS "procured Facebook to track and intercept Plaintiff's . . . internet communications while navigating their websites." FAC ¶ 62. The Complaint fails to state a WESCA claim, for numerous reasons.

A. Plaintiff Does Not Allege That An Interception Occurred In Pennsylvania.

As an initial matter, Plaintiff fails to allege that a WESCA violation occurred in Pennsylvania. The WESCA applies only to "interceptions" that occur in Pennsylvania. *See Larrison v. Larrison*, 750 A.2d 895, 898 (Pa. Super. Ct. 2000) (not "extend[ing] the WESCA to cover conduct occurring wholly outside the Commonwealth"); *Popa v. Harriet Carter Gifts, Inc.*, 52 F.4th 121, 132 (3d Cir. 2022) (explaining that because the Commonwealth can only control the activities that occur within its borders, it must look to the place of interception). Where interceptions occur on a website, the "place of interception is the point at which the signals were routed to [a third party's] servers." *Popa*, 52 F.4th at 132.

Here, Plaintiff does not allege the location where his information was routed to Facebook's servers. Even so, the Complaint is clear that the pixel on Cabela's website apparently caused the interception, which means the point where Plaintiff's information was routed to Facebook is where Plaintiff alleges the interception occurred. *See* FAC ¶ 17 (Cabela's website servers hosted the pixel code that was

"configured to transmit . . . events to Facebook."); *see also id.* ¶ 14 ("[w]hen the Facebook Tracking Pixel captures an action, it sends a record to Facebook."); *id.* ¶ 62 (BPS "sent these communications to Facebook"). Plaintiff's Amended Complaint, including his new allegation that he was in Pennsylvania at the time he accessed Cabela's website and completed his purchase, does not change the place of interception. *See id.* ¶ 6. This fundamental deficiency is fatal. Although the Court must accept Plaintiff's factual allegations as true, the Court cannot accept facts where none are alleged. *See Scott v. Clark*, 2020 WL 4905624, at *1 (W.D. Pa. July 28, 2020) (dismissing claims because the court cannot "accept inferences drawn by a plaintiff if they are unsupported by the facts in the complaint"); *see also Popa*, 52 F.4th at 131–32 (refusing to assume that because Popa was a Pennsylvania citizen, the place of interception was also in Pennsylvania, as the Complaint does not identify where the "JavaScript began telling the browser to communicate with its servers").

For this reason alone, Plaintiff fails to state a valid claim under the WESCA.

B. Plaintiff Fails to Allege Electronic Communications Were "Intercepted."

Even if Plaintiff had alleged that the relevant conduct occurred in Pennsylvania, his WESCA claim still fails. Plaintiff does not allege several of the key elements of an "interception," including an interception or acquisition (1) of any "**contents**" of Plaintiff's communications with BPS or (2) through the use of a "**device**," as required by the WESCA. *See* 18 Pa.C.S. § 5702.

1. Plaintiff does not Allege that the "Contents" of his Communications with BPS were Intercepted.

Not all data related to communications triggers the WESCA. The interception at issue must be communication of "contents." Contents means "information concerning the substance, purport, or meaning of that communication." 18 Pa.C.S. § 5702. In other words, the defendant must capture "the intended message conveyed by the communication," like the text of an email message or words spoken on a call. *In re Zynga Priv. Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014). Information that does not convey the intended message does not constitute contents under the Act. *See In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 135–39 (3d Cir. 2015) (identifying the differences between content and record information); *see also In re Zynga Privacy Litig.*, 750 F.3d at 1106–07 ("Contents" does not include information "generated in the course of the communication").[3]

Here, Plaintiff alleges the Facebook Pixel on Cabela's website had the ability to capture the URLs of webpages visited, the title and description of the webpages, button clicks, and form-field information collected through the button click tool and Facebook's advanced matching feature. FAC ¶¶ 18–25, 32. Plaintiff does not allege what URLs he visited, what buttons he clicked, or any forms he completed on Cabela's website. Nor does he allege that any form-field information was actually

[3] Courts generally interpret the federal Wiretap Act and the WESCA "in the same way." *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 113 n.6 (3d Cir. 2003).

sent to Facebook in plain text. Instead, the Amended Complaint shows that any form-field information was "hidden," *see id.* ¶ 24, or hashed before it was sent to Facebook. *Id.* ¶ 32. Even so, Plaintiff summarily alleges that BPS procured Facebook to intercept his "internet communications while navigating its websites." *Id.* ¶ 62. But even if Plaintiff adequately alleged specific internet communications of his that were intercepted, the type of information Cabela's website allegedly sent to Facebook is not "content." Instead, the information Plaintiff alleges Cabela's sent to Facebook is non-content "dialing, routing, addressing, or signaling" information. *In re Google Inc.*, 806 F.3d at 137; *see also* Compl. ¶¶ 15–16, 18–26, 32.

First, a URL, or a Uniform Resource Location, is not "content." A URL is instead a "file path" to take a webpage visitor to a particular location, *i.e.*, a "file contained in a folder on a web server owned or operated by [the defendant]," that is "used to identify the physical location of documents on servers connected to the internet." *In re Nickelodeon Consumer Priv. Litig.*, 2014 WL 3012873, at *15 (D.N.J. July 2, 2014) (internal quotation marks omitted). For example, the URL for Cabela's website is https://www.cabelas.com. This data plainly reflects a "dialing, routing, addressing, or signaling" function, not the substance written in a communication. *In re Google*, 806 F.3d at 137. Likewise, the title and description of a webpage merely describe "addressing" information, not the substance of any purported communication to BPS. As courts have found, this type of addressing

information has "less in common with 'the spoken words of a telephone call,' than [it] do[es] with the telephone number dialed to initiate the call," because they are "static descriptions more akin to 'identification and address information.'" *In re Nickelodeon*, 2014 WL 3012873, at *15 (rejecting any argument that a URL was a "contents" for wiretapping purposes) (citations omitted)).

For the same reasons URLs do not disclose the "contents" of a communication, neither do button clicks or form-field information, like a person's name, address, or contact information. Federal courts have specifically found that the identities of the parties to a communication and their addresses are not content. *See In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1061 (N.D. Cal. 2012) ("[I]dentities of parties to a communication . . . is not 'content' as defined by the Wiretap Act" because such data "contains no information concerning the substance, purport, or meaning of [the] communication.") (internal quotation marks omitted); *see also Graham v. Noom, Inc.*, 533 F. Supp. 3d 823, 833 (N.D. Cal. 2021) ("Content" does not include information "generated in the course of the communication," including the "name, address and subscriber number or identity of a subscriber or customer"); *see also Goldstein v. Costco Wholesale Corp.*, 559 F. Supp. 3d 1318, 1321–22 (S.D. Fla. 2021) (holding mouse movements, clicks, pages visited, and keystrokes, including information allegedly input by the plaintiff, were not "contents" under FSCA).

The fact that this information is not content is consistent with Facebook's alleged use of the data. Plaintiff's own allegations are that the information from BPS is compiled "into a generalized dataset." FAC ¶ 12; *see also In re Meta Pixel Healthcare Litig.*, 2022 WL 17869218 *2 (N.D. Cal. Dec. 22, 2022). Given that the information allegedly disclosed to Facebook by BPS does not contain PII and is later used in a generalized, anonymized form, the information cannot be content that Plaintiff would expect to remain private. *See Massie v. Gen. Motors LLC*, 2022 WL 534468, at *5 (D. Del. Feb. 17, 2022) ("[T]here is no expectation of privacy over anonymized data captured by [] software.").

In sum, the information Plaintiff alleges was disclosed is exactly the type of non-content record information that courts recognize does not support a WESCA violation. As a result, Plaintiff's claim should be dismissed.

2. **Facebook Pixel is not a "Device."**

Plaintiff alleges "a piece of code" intercepted his electronic communications. FAC ¶ 14 ("The Facebook Tracking Pixel is a piece of code"). But software code on a website—which is all that the Facebook Pixel is—is not a "device" within the term's statutory definition. The WESCA defines "device" to include "[a]ny device or apparatus, including, but not limited to, an induction coil or a telecommunication identification interception device, that can be used to intercept a wire, electronic or oral communication." 18 Pa.C.S. § 5702. Under their plain and ordinary meanings,

a "device" or "apparatus" must be tangible; a device does not encompass intangible software code on a website. *See* Black's Law Dictionary (11th ed. 2019) (defining "device" as "[a] mechanical invention" that may be "an apparatus or an article of manufacture," and defining "apparatus" with reference to "machine," which is defined as "[a] device or apparatus consisting of fixed and moving parts"). As such, Pennsylvania courts require an interception to occur through a tangible device. *See*, *e.g.*, *Com. v. Mason*, 247 A.3d 1070, 1081–82 (Pa. 2021) (discussing the use of a nanny cam to intercept conversations); *Com v. Diego*, 119 A.3d 370, 376 (Pa. Super. Ct. 2015) (finding an iPad is an "electronic, mechanical, or other device"); *Com. v. Parrella*, 610 A.2d 1006, 1009–10 (Pa. Super. Ct. 1992) (finding use of a baby monitor and tape recorder fits the meaning of "device").

Indeed, consistent with this plain meaning, numerous other courts have found that computer code cannot be not a "device" or "apparatus" under similar wiretap laws. *See*, *e.g.*, *Potter v. Havlicek*, 2008 WL 2556723, at *8 (S.D. Ohio June 23, 2008) (dismissing federal wiretap claim because "the word 'device' does not encompass software"); *Jacome v. Spirit Airlines*, 2021 WL 3087860, at *5 (Fla. Cir. Ct. June 17, 2021) (dismissing Florida wiretap claim because session replay software is not a "device or apparatus"); *Cardoso v. Whirlpool Corp.*, No. 21-CV-60784-WPD, 2021 WL 2820822, at *2 (S.D. Fla. July 6, 2021) (same); *Connor v. Whirlpool Corp.*, 2021 WL 3076477, at *2 (S.D. Fla. July 6, 2021) (same); *cf. United States v.*

Ackies, 918 F.3d 190, 199 n.5 (1st Cir. 2019) (rejecting argument that software is a "device" under Federal Stored Communications Act); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 972 (S.D. Cal. 2012) ("[S]oftware is not a tangible good or service."). Because Plaintiff does not even attempt to allege the interception occurred through a tangible device, the Court should dismiss the WESCA claim.

C. Plaintiff consented to any alleged interception.

Most fundamentally, Plaintiff's WESCA claim is deficient because Plaintiff consented to the alleged interception. The mutual consent exception applies where "all parties to the communication have given prior consent to such interception." 18 Pa.C.S. § 5704(4). In Pennsylvania, prior consent does not require actual knowledge by a plaintiff that he was being recorded; a person consents to an interception where they are given notice but choose to proceed anyway. *See Popa*, 52 F.4th at 132 (the mutual consent exception does not require "actual knowledge"); s*ee also Commonwealth v. Byrd*, 185 A.3d 1015, 1022–23 (Pa. Super. 2018) (a person cannot avoid consent by ignoring an audio recording warning that a call may be recorded). Despite now claiming otherwise, Plaintiff plainly consented to the alleged interception—both by accepting Facebook's written policies and through his choice to use of Cabela's website despite Cabela's clear, public notice that the website uses pixels for advertising purposes.

1. Plaintiff consented to the alleged interception by accepting Facebook's policies.

As an "active Facebook user," the fact that Facebook collects Plaintiff's information—including from third-party websites—should not come as a surprise. FAC ¶ 14. Facebook users, like Plaintiff, consent to the transmission and use of their data by Facebook when they accept Facebook's policies at the time they sign up for Facebook.[4] *Id.* ¶ 40.

As Facebook's policies explain, Facebook collects data about individuals' browsing activities across the Internet—known as "off-Facebook activity"—through cookies and tools like the Facebook pixel. Ex. A (Facebook's Cookies Policy); s*ee also* FAC ¶ 12 (explaining that "Facebook can target users so effectively because it surveils user activity both on and off its site."); *see also id.* ¶ 42 (Facebook acknowledged that "[p]artners receive your data when you visit or use their services or through third parties they work with."). This includes information about the user's interactions with the websites they visit. Facebook collects this information to enable

[4] Plaintiff refers to and relies upon Facebook's policies in his Complaint, this includes the Terms of Service, the Cookies Policy, and the Data Policy. *See*, *e.g.*, FAC ¶ 40. As a result, this Court may consider the policies in ruling on BPS's motion to dismiss. *See e.g.*, *In re Burlington Coat Factory Sec. Litig.*, 114 F.3d 1410, 1426 (3d Cir. 1997) (In ruling on a motion to dismiss, a court may consider a "document *integral to or explicitly relied* upon in the complaint." (citations omitted, emphasis in original)); *ALA, Inc. v. CCAIR, Inc.*, 29 F.3d 855, 859 (3d Cir. 1994) (same); *Fallon v. Mercy Cath. Med. Ctr. of Se. Pa.*, 877 F.3d 487, 493 (3d Cir. 2017) (same).

advertisers to reach the "people who have already shown an interest in [their] business." *Id.* ¶ 13. Courts have found similar Facebook disclosures to be adequate to constitute notice to Facebook users of its tracking activity. *See Smith v. Facebook, Inc.*, 262 F. Supp. 3d 943, 954–55 (N.D. Cal. 2017) (finding Facebook's policies disclose "the precise conduct at issue" and therefore constitute adequate notice).

Even so, if a Facebook user chooses, they may adjust their account settings to stop Facebook from tracking their off-Facebook activity. *See id.* ¶ 43; Ex. A (Facebook's Cookies Policy); *see* Ex. B ("Off-Facebook Activity: Control your information"); *see also* Ex. C (Facebook Help Center: "How do I manage my future off-Facebook activity"). In addition, Plaintiff can also control whether his own browser retains any cookies. *See* Ex. A (Facebook's Cookies Policy) ("[Y]our browser or device may offer settings that allow you to choose whether browser cookies are set and to delete them"). Here, Plaintiff took no such steps to stop Facebook from monitoring his off-Facebook activity.

By continuing to use Facebook and accepting its policies, Plaintiff consented to the alleged disclosure of his website activities to Facebook. *See Popa* 52 F.4th at 132 ("Prior consent, including implied consent, can be demonstrated when the person being recorded knew or should have known that the conversation was being recorded.") (citation and bracket omitted)).

2. **Plaintiff consented to BPS's use of the Facebook Pixel by accepting the terms of BPS's Privacy Policy.**

Plaintiff consented to BPS's use of the Facebook Pixel by accepting BPS's privacy policy. Plaintiff now alleges that BPS's privacy policy failed to disclose that BPS "assist[s] Facebook with intercepting communications." FAC ¶ 38. Yet in no uncertain terms, BPS's publicly-posted privacy policy notifies website users that the company "may use third party-placed tracking pixels and Cookies and related or similar technologies to help us understand how to improve the customer experience on our Sites, to personalize our content, and to develop and improve our products and services, including advertising." BPS's Privacy and Security Statement, https://www.basspro.com/shop/en/privacy-policy-summary-bass-pro-shops (eff. Sept. 17, 2020).[5] BPS's privacy statement continues, stating that the company "ha[s] collected the following categories of information from the listed sources, used it for the listed business purposes and shared it with the listed categories of third parties." *Id.* Within that list, BPS identifies:

Category Of Information	**Collected?**	**Source**	**Business purposes* for use**
Identifiers (name, alias, postal address, email address, phone number, fax number, account name, Social Security	Individuals submitting information to us; information	Auditing relating to transactions; security detection, protection and	Service providers and others, such as payment processors,

[5] A single privacy policy applies to all mobile applications, websites, and domains owned by the Bass Pro family of companies, which includes Bass Pro Shops and Cabela's. Webpage from Oct. 27, 2021 archived at https://web.archive.org/web/20220625161219/https://www.basspro.com/shop/en/privacy-policy-summary-bass-pro-shops.

number, driver's license number, passport number, unique personal identifier, IP address)	we automatically collect from site visitors; information we may receive from third parties.	enforcement; functionality debugging/error repair; ad customization; performing services for you; internal research and development; quality control.	mail houses, marketing partners, shipping partners, employee benefits partners, analytics partners; affiliated companies; government regulators; law enforcement; strategically aligned businesses.
***			
Commercial information (transaction history, products/services purchased, obtained or considered, product preference)	Individuals submitting information; information we automatically collect from site visitors; information we may receive from third-party marketing or data partners.	Auditing relating to transactions; security detection, protection and enforcement; functionality debugging/error repair; ad customization; performing services for you; internal research and development; quality control.	Service providers and others, such as payment processors, mail houses, marketing partners, shipping partners, analytics partners; affiliated companies; government regulators; law enforcement; strategically

			aligned businesses.
Electronic network activity (browsing or search history, website interactions, advertisement interactions)	Information automatically collected from site visitors.	Auditing relating to transactions; security detection, protection and enforcement; functionality debugging/error repair; ad customization; performing services for you; internal research and development; quality control.	Service providers and others, such as advertising and analytics partners; affiliated companies; law enforcement.

Id.

The privacy statement then goes on to state that "the business purposes" for which the identified information is used, including browsing and website interactions, may include (1) "[p]erforming services" for its customers and website users; (2) "[a]dvertising customization"; (3) "[a]uditing relating to transactions, internal research and development," including for "troubleshooting [and] Site customization"; (4) "[s]ecurity detection, protection and enforcement; functionality debugging, error repair"; (5) "[d]ispute resolution"; and (6) "[q]uality control[.]" *Id.*

Thus, BPS's privacy statement disclosed the potential collection of data associated with a website user's browsing activity and website interactions through third-party pixels. A reasonable person browsing Cabela's website would be alerted

to the privacy statement and its bolded provisions directly applicable to Plaintiff's claims here. At any rate, regardless of BPS's privacy policy, Plaintiff consented to the alleged capture of data here because "[a]ny reasonably intelligent person, savvy enough to be using the Internet," would be aware that to conduct an online search or click a webpage link requires her computer to send that query over the public internet to retrieve the webpage and that such transmissions "are received in a recorded format, by their very nature." *Commonwealth v. Proetto*, 771 A.2d 823, 829 (Pa. Super. 2001), *aff'd*, 837 A.2d 1163 (Pa. 2003).

Plaintiff cannot bring a claim under the WESCA for conduct to which he consented. Whether he actually reviewed the privacy statement is of no consequence. *See Popa*, 52 F.4th at 132. But because Plaintiff proceeded to use Cabela's website in spite of his knowledge that his online interactions would be recorded based on Cabela's express disclosures on its website that his communications would be recorded, he consented by proceeding to use Cabela's website. *See Popa* 52 F.4th at 132. Plaintiff's WESCA claim should be dismissed.

III. Plaintiff's Claim Under the Uniform Firearms Act Fails.

Pennsylvania's Uniform Firearms Act states that "[a]ll information provided by [a] potential purchaser . . . including, but not limited to [the potential purchaser's] name or identity, furnished by a potential purchaser . . . under this section . . . shall be confidential and not subject to public disclosure." 18 Pa.C.S. § 6111(i). Plaintiff

claims BPS violated this statute by sharing information about Plaintiff's alleged firearm purchase with Facebook. Plaintiff's claim fails for numerous reasons.

A. Plaintiff has not alleged an improper "disclosure."

The UFA prohibits the "disclosure" of information about an individual's firearm purchase. Here, however, Plaintiff does not clearly allege that *BPS* made any public disclosure to Facebook. Indeed, with respect to his WESCA claim, Plaintiff alleges that BPS "assisted Facebook" with supposedly intercepting his communications. FAC ¶¶ 9, 38. Yet, with respect to his UFA claim, Plaintiff makes a single conclusory allegation that "Defendants disclosed to Facebook information that Plaintiff provided to them in connection with his purchase of these firearms." *Id.* ¶ 70. BPS cannot simultaneously be the party responsible for "intercepting" a communication and also for "procuring" Facebook to commit an interception.

Adding to the confusion, the Complaint also alleges that Plaintiff's own browser—not BPS—disclosed information to Facebook. FAC ¶ 28 ("[T]he Facebook Tracking Pixel compels the user's browser" to send cookie information to Facebook). This allegation demonstrates not only that BPS is not making the alleged "disclosure," but also that any personally identifying information comes from the cookies maintained on Plaintiff's browser—and not BPS.

While this Court must accept "all well-pleaded factual allegations in the complaint as true, it need not accept allegations that are internally inconsistent or

contradict matters of public record." *Amelio v. McCabe, Weisberg & Conway, P.C*, 2015 WL 4545299, at *4 (W.D. Pa. July 28, 2015); *see also Bocker v. Hartzell Engine Techs., LLC*, 2023 WL 415792, at *4 (D. Del. Jan. 26, 2023) ("[T]he court is not obligated to reconcile or accept such contradictory allegations."). Plaintiff's inconsistent and contradictory allegations about *who* made the supposedly improper disclosure to Facebook are not enough to sustain his claim.

B. Plaintiff does not allege that BPS disclosed information "furnished" under the UFA.

Not all information is regulated by the confidentiality provision of the UFA. The UFA prohibits only the public disclosure of information which was "**furnished** by a potential purchaser or transferee **under this section**," referring to Pennsylvania Statute Section 6111. 18 Pa.C.S. § 6111 (emphasis supplied). And under Section 6111(b), the only potential information to be "furnished" is an "application/record of sale." 18 Pa.C.S. § 6111(b)(1). Here, however, Plaintiff does not allege he completed an application or record of sale, or that form to BPS on Cabela's website. And he certainly does not allege that BPS disclosed an application of record or sale under Section 6111. The fact that Plaintiff alleges BPS disclosed other information related to his firearm purchase makes no difference—the confidentiality provision of the UFA only applies to an "application/record of sale," which is simply not at issue here. Plaintiff's WESCA claim should be dismissed.

C. Plaintiff does not allege a "public" disclosure.

Even if there were an improper "disclosure" here, Plaintiff does not allege a "public" disclosure as required by the statute's plain text. *See* 18 Pa.C.S. § 6111(i). Plaintiff fails to allege a public disclosure for at least two reasons. First, the alleged disclosure was not "public"—if anything, Plaintiff alleges a private disclosure, to a single entity, Facebook. Plaintiff does not allege anyone at Facebook actually saw his information, let alone that that numerous individuals at Facebook did. Plaintiff's allegations are far from the required "public" disclosure. Second, the Commonwealth Court of Pennsylvania has held that a person violates Section 6111(i) by "revealing an applicant's name or identity to a person not . . . ***otherwise authorized by an applicant***." *Doe v. Franklin Cnty.*, 139 A.3d 296, 307 (Pa. Commw. Ct. 2016) (emphasis supplied), *rev'd on other grounds*, 644 Pa. 1, 174 A.3d 593 (2017). Here, Plaintiff does not allege that his "name or identity" was disclosed to a person not "authorized by" Plaintiff to receive it. As discussed above, Plaintiff gave his consent to Facebook to gather information about his web browsing activities. *See supra*, Section I.C. Thus, Plaintiff has not alleged that his information was disclosed to a person not "otherwise authorized by an applicant" to receive it. *Franklin Cnty.*, 139 A.3d at 307. Plaintiff's claim fails on its face.

CONCLUSION

Plaintiff's Amended Complaint should be dismissed.

SHOOK, HARDY & BACON L.L.P.

Dated: July 14, 2023

By: */s/ Erin L. Leffler*

Erin L. Leffler (PA ID No. 204507)
SHOOK, HARDY & BACON L.L.P.
Two Commerce Square
2001 Market St., Suite 3000
Philadelphia, PA 19103
Tel: (215) 278-2555
eleffler@shb.com

Jennifer A. McLoone (*pro hac vice*)
SHOOK, HARDY & BACON L.L.P.
201 South Biscayne Blvd., Suite 3200
Miami, FL 33131
Tel: (305) 358-5171
jmcloone@shb.com

Anna A. Gadberry (*pro hac vice*)
SHOOK, HARDY & BACON L.L.P.
2555 Grand Boulevard
Kansas City, MO 64108
Tel: (816) 474-6550
agadberry@shb.com

Lindsey M. Knapton (*pro hac vice*)
SHOOK, HARDY & BACON L.L.P.
1600 17th Street, Suite 450
Denver, CO 80202
Tel: (303) 285-5300
lknapton@shb.com

Attorneys for Defendants Cabela's L.L.C. and BPS Direct, L.L.C.